

GENERAL			
<b>This document is under the Change Management Control Policy.</b>			
<b>Description</b>	This document establishes an Availability Management process and procedures for Fermilab.		
<b>Purpose</b>	The purpose of this document is to describe the top-level Availability Management process and define the activities for each sub-process area. Four sub-process areas make up the Availability Management Process as described later in this document.		
<b>Applicable to</b>	<i>All processes and services</i>		
<b>Supersedes</b>	N/A		
<b>Document Owner</b>	Availability Manager	<b>Owner Org</b>	Computing
<b>Effective Date</b>	2010-09-21	<b>Revision Date</b>	At minimum annually

VERSION HISTORY			
Version	Date	Author(s)	Change Summary
1.0	2010-09-21	Matt Crawford	Initial approved document
2.0	2011-12-20	Matt Crawford	Annual review & revision
2.1	2012-08-12	Rick Snider	Update procedures to reflect what we are actually doing with Availability.
3.0	2012-09-05	Tammy Whited	Review and approve changes.
3.1	2012-11-30	Jack Schmidt	Standardize KPI reports
4.0	2015-09-29	Anthony Donzelli	Adjusted sections 1.1-1.5 to reflect the current state of work. All sections were updated. Added the Communication Plan to the appendix.
4.1	2016-10-19	Anthony Donzelli	Annual review & revision
4.2	2017-10-17	Anthony Donzelli	Added Appendix 4
4.3	2018-09-25	Anthony Donzelli	Annual review & revision
4.4	2019-11-5	Anthony Donzelli	Updated Narratives 1.1-1.5 to include Service Owners alongside Availability Manager.

4.5	2020-9-23	Anthony Donzelli	Annual review & revision
-----	-----------	------------------	--------------------------

## TABLE OF CONTENTS

<b>GENERAL</b> .....	1
<b>VERSION HISTORY</b> .....	1
<b>EXECUTIVE OVERVIEW – AVAILABILITY MANAGEMENT</b> .....	5
<b>PROCESS CONTEXT DIAGRAM – AVAILABILITY MANAGEMENT</b> .....	6
<b>PROCESS FLOW – AVAILABILITY MANAGEMENT</b> .....	7
<b>ROLES AND RESPONSIBILITIES – AVAILABILITY MANAGEMENT</b> .....	7
<b>PROCESS MEASUREMENTS</b> .....	8
<b>1.1 MONITOR AND REVIEW PROCEDURE FLOW</b> .....	8
1.1 MONITOR AND REVIEW ENTRY CRITERIA – AVAILABILITY MANAGEMENT.....	9
REVIEW CURRENT AVAILABILITY NARRATIVE.....	10
REVIEW CURRENT AVAILABILITY EXIT CRITERIA, OUTPUTS.....	11
REVIEW CURRENT AVAILABILITY RISKS.....	11
<b>1.2 INVESTIGATE AND REMEDIATE PROCEDURE FLOW</b> .....	13
1.2 INVESTIGATE AND REMEDIATE ENTRY CRITERIA – AVAILABILITY MANAGEMENT .....	13
1.2 INVESTIGATE AND REMEDIATE NARRATIVE .....	15
1.2 INVESTIGATE AND REMEDIATE EXIT CRITERIA, OUTPUTS .....	15
1.2 INVESTIGATE AND REMEDIATE RISKS.....	16
<b>1.3 PLAN AND DESIGN PROCEDURE FLOW</b> .....	17
1.3 PLAN AND DESIGN ENTRY CRITERIA – AVAILABILITY MANAGEMENT .....	17
1.3 PLAN AND DESIGN NARRATIVE .....	19
DOCUMENT NEW REQUIREMENTS EXIT CRITERIA, OUTPUTS.....	19
DOCUMENT NEW REQUIREMENTS RISKS .....	20
<b>1.4 EXECUTE RISK MANAGEMENT FLOW</b> .....	21
EXECUTE RISK MANAGEMENT ENTRY CRITERIA – AVAILABILITY MANAGEMENT .....	22
EXECUTE RISK MANAGEMENT NARRATIVE .....	22
EXECUTE RISK MANAGEMENT EXIT CRITERIA, OUTPUTS .....	22
EXECUTE RISK MANAGEMENT RISKS.....	23
<b>1.5 SERVICE CAPABILITIES FLOW</b> .....	24
IMPLEMENT NEW AVAILABILITY ENTRY CRITERIA – AVAILABILITY MANAGEMENT .....	26
IMPLEMENT NEW AVAILABILITY NARRATIVE.....	26
IMPLEMENT NEW AVAILABILITY EXIT CRITERIA, OUTPUTS .....	26
IMPLEMENT NEW AVAILABILITY RISKS.....	27
<b>PROCESS INTEGRATION POINTS – AVAILABILITY MANAGEMENT</b> .....	28
<b>SUPPORTING DOCUMENTS</b> .....	30
<b>APPENDIX 1 - AVAILABILITY RACI MATRIX</b> .....	31
<b>APPENDIX 2 – COMMUNICATION</b> .....	33
<b>APPENDIX 3 - DEFINITIONS</b> .....	34

---

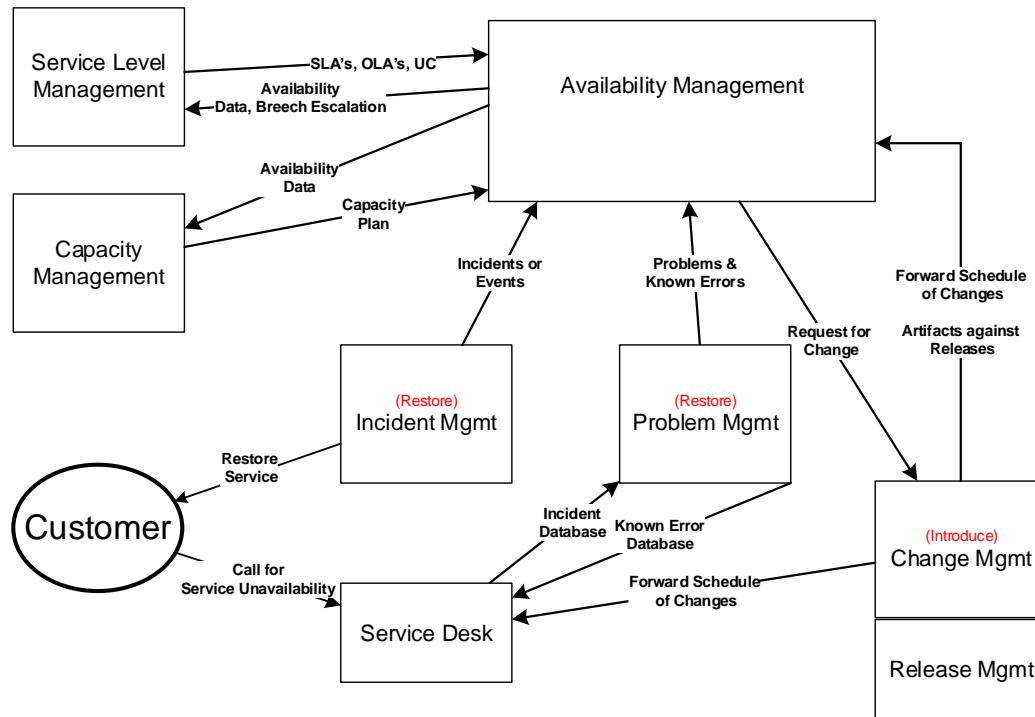
<b>APPENDIX 4 – ISO REQUIREMENTS .....</b>	<b>34</b>
--	-----------

## EXECUTIVE OVERVIEW – AVAILABILITY MANAGEMENT

Goal	<ul style="list-style-type: none"><li>• ISO/IEC 20000 defines Availability as the ability of a component or service to perform its agreed function when required. More specifically, Availability Management has two main focuses:<ul style="list-style-type: none"><li>○ Infrastructure components which are required to meet all Service Level Agreements (SLA's) in the organization,</li><li>○ Infrastructure components which are required to support the organization's Critical Business Functions.</li></ul></li></ul>
Benefits	<ul style="list-style-type: none"><li>• Improved customer, business and user satisfaction</li><li>• Cost effective management of the IT services to meet the business needs,</li><li>• Reduction in the frequency and duration of the IT service failures,</li><li>• A transformation from a reactive to a pro-active IT mindset</li><li>• Availability management underpins service level management</li><li>• IT becomes more proactive in providing support to the business.</li></ul>

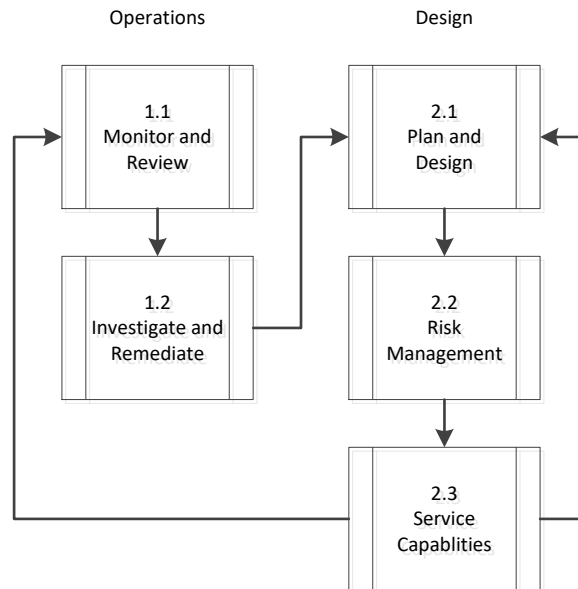
## PROCESS CONTEXT DIAGRAM – AVAILABILITY MANAGEMENT

### HIGH LEVEL INTERFACING PROCESS FLOW



NOTE: This graphic illustrates the basic interactions between this process or functions and the ITIL processes at a high level and does not represent detailed dependencies.

## PROCESS FLOW – AVAILABILITY MANAGEMENT



## ROLES AND RESPONSIBILITIES – AVAILABILITY MANAGEMENT

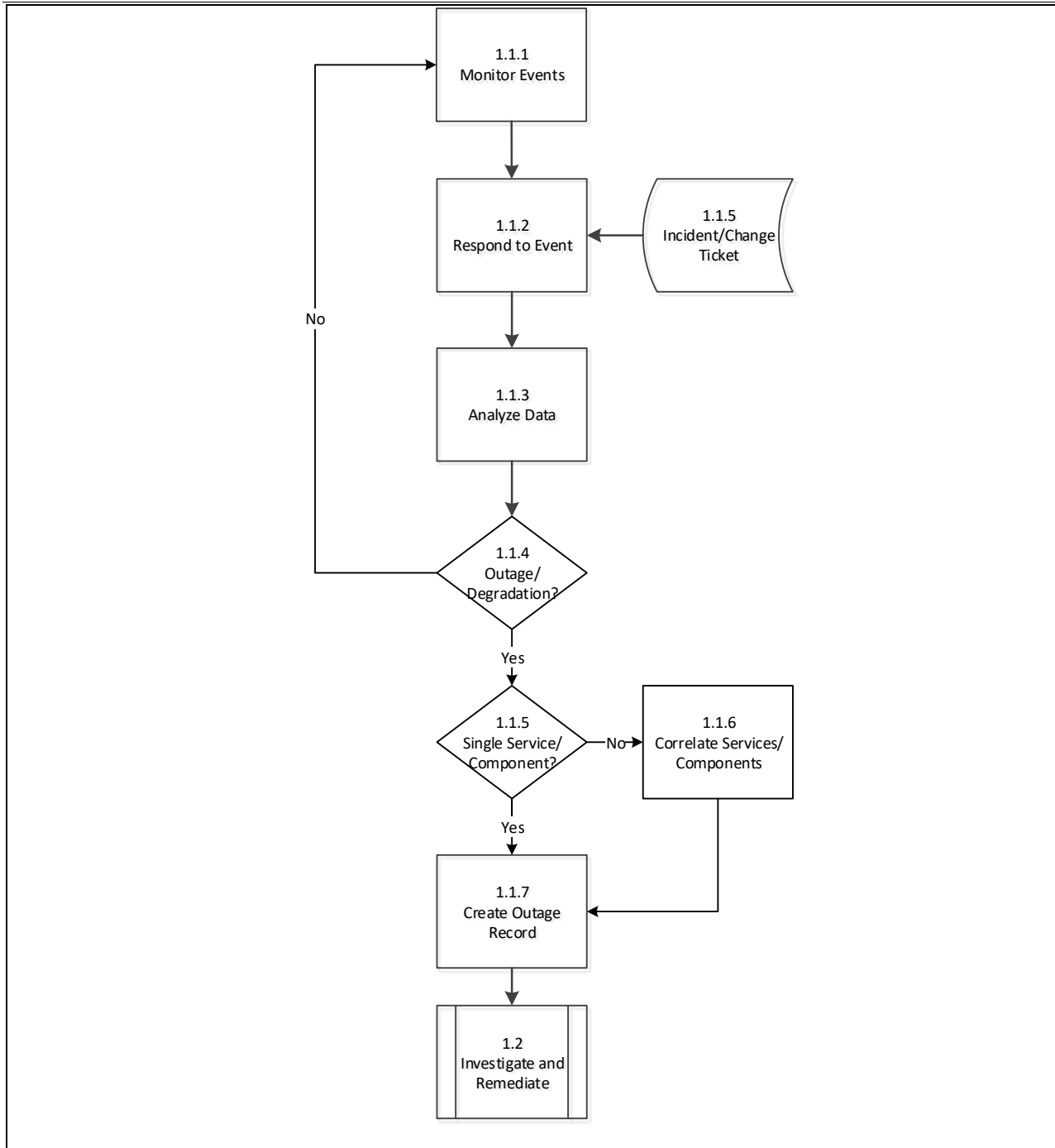
Roles	Responsibilities
Availability Manager	<ul style="list-style-type: none"> <li>Monitor, measure, analyze, reporting and reviewing service and component availability</li> <li>Investigate service and component unavailability and initiate remedial action</li> <li>Plan and design new or changed services</li> <li>Determine the vital business functions, availability requirements and targets</li> <li>Perform risk management activities</li> <li>Manage and monitor Outage record creation</li> </ul>
Incident Manager	<ul style="list-style-type: none"> <li>Inform/Record Availability events to the Availability Manager</li> </ul>
Service Level Manager	<ul style="list-style-type: none"> <li>Receive management information such as SLA Breach targets and data from AM.</li> <li>Provide availability SLA's, OLA's, UC to Availability Manager.</li> </ul>
Tier 1 (Service Desk)	<ul style="list-style-type: none"> <li>Detect possible availability events and escalate them to Tier 2 Support Staff for Outage record creation.</li> </ul>

<b>ROLES AND RESPONSIBILITIES – AVAILABILITY MANAGEMENT</b>	
<b>Roles</b>	<b>Responsibilities</b>
Tier 2 (Operations) Support Staff	<ul style="list-style-type: none"> <li>Plan and design new or changed services</li> <li>Determine the vital business functions, availability requirements and targets</li> <li>Perform risk management activities</li> <li>Manage and record Outage record creation</li> </ul>
Stakeholders	<ul style="list-style-type: none"> <li>Participate in audits, reviewing results of the audit &amp; performing corrective actions.</li> </ul>

<b>PROCESS MEASUREMENTS</b>				
<b>Key Performance Indicators</b>	<b>Frequency</b>	<b>Upper/Lower Control Limits</b>	<b>Objectives</b>	<b>Data Captures</b>
Report IT Service Availability	Weekly	90% minimum availability target	Reported in weekly operations meetings in Availability chart, along with any incidents associated with availability breaches.	Weekly Operations Report
Availability reviews	Annually		Ensure that availability targets and plans are reviewed at least annually.	Service Level Dashboards
Number of service improvements based on availability identified	Monthly		Track service improvements based on Availability requirements	Service Now Dashboards

## 1.1 MONITOR AND REVIEW PROCEDURE FLOW





### 1.1 Monitor and Review Entry Criteria – Availability Management

<b>Inputs</b>	<ul style="list-style-type: none"> <li>• 'Threshold' event</li> <li>• Incident Report</li> <li>• SLA breaches</li> </ul>
---------------	--

<b>Entry Criteria</b>	<ul style="list-style-type: none"> <li>• Performance Incident escalated by Incident Management</li> <li>• Availability Problem escalated by Problem Management</li> <li>• Service breach</li> </ul>
<b>General Comments</b>	<ul style="list-style-type: none"> <li>• Data collection needs to be across all the Configuration Items that make up the Service end-to-end so that a holistic picture of Service performance can be documented and understood.</li> <li>• Analysis of the data collected from the monitoring procedure (along with data provided by Incident Management) will allow for a comparison between the current performance of the IT environment and its expected performance as documented in SLAs.</li> </ul>

<b>Review Current Availability Narrative</b>		
<b>Step</b>	<b>Responsible Role</b>	<b>Action</b>
1.1.1	Availability Manager	<ul style="list-style-type: none"> <li>• Monitor according to SLA requirements (i.e. at points and over time periods consistent with reporting of Availability Targets as required by the Business (Critical Business Functions), users (IT Services), and to the IT Support Organization (enabling-Components). Monitoring includes: <ul style="list-style-type: none"> <li>○ Network</li> <li>○ Authentication</li> <li>○ Infrastructure (Middleware, Storage, Database, Server)</li> <li>○ Application</li> <li>○ Functional Services</li> <li>○ Operations Reports</li> </ul> </li> </ul>
1.1.2	Availability Manager	<ul style="list-style-type: none"> <li>• Receive information from possible Availability events from Incident and/or Change records, telephone, walk-up, email, etc.</li> <li>• Coordinate with Incident, Change Manager and/or Service Provider to validate an event occurred</li> <li>• Update the Incident and/or Change Record with information as necessary</li> </ul>
1.1.3	Availability Manager/ Tier 2 Support Teams	<ul style="list-style-type: none"> <li>• Acquire all the information needed, and possible, to ensure effective analysis</li> </ul>

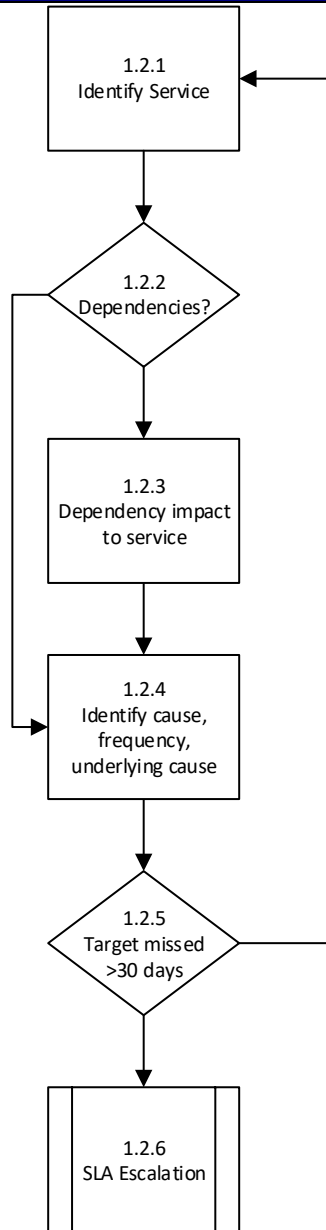
Review Current Availability Narrative		
Step	Responsible Role	Action
1.1.4	Availability Manager/Service Owner	Has an Outage or Degradation occurred? <ul style="list-style-type: none"> <li>Validate against service outage definition, criticality and service hours and move to step 1.1.5</li> <li>If there is no Outage or Degradation, go to step 1.1.1</li> </ul>
1.1.5	Availability Manager/Service Owner	Validate using BSM Maps and Availability Reports to determine services/components impacted <ul style="list-style-type: none"> <li>Is more than one service/component impacted? Go to step 1.1.6</li> <li>If only one service/component impacted, go to step 1.1.7</li> </ul>
1.1.6	Availability Manager/Service Owner	Correlate Services and Components impacted by the Outage/Degradation by using CI relationships and dependencies and prepare to record Outage/Degradation data for each
1.1.7	Availability Manager/Service Owner	Create an Outage Record for any impacted Services/Components including: <ul style="list-style-type: none"> <li>Service Offering</li> <li>Task Number</li> <li>Type</li> <li>Duration</li> </ul>

Review Current Availability Exit Criteria, Outputs	
<b>Outputs</b>	<ul style="list-style-type: none"> <li>Routine monitoring completed for defined timescale</li> <li>Completed data analysis</li> <li>New Outage Record</li> </ul>
<b>Exit Criteria</b>	<ul style="list-style-type: none"> <li>Outage Record created with information complete</li> </ul>

Review Current Availability Risks	
Risk	Impact
Availability Management not engaged in an Incident/Event in a timely manner	Reduced opportunity for necessary technical expertise to be applied

Review Current Availability Risks	
Risk	Impact
	Reduced opportunity for necessary actions to be undertaken
Monitoring is not undertaken to the required level of detail	Relevant data is not collected which can lead to an inability to proactively prevent Availability- and Performance-related Incidents Optimization opportunities are lost
Monitoring is not undertaken at the Service and component levels	A holistic picture of Service performance cannot be documented and understood
Thresholds are incorrectly set	Relevant data is not collected which can lead to an inability to proactively prevent Availability- and Performance-related Incidents Too many or too few alarms are generated and support staff miss genuine issues
Incomplete analysis	Incomplete analysis would not allow full understanding of any performance differences between the current and expected IT environment
Inadequate cross-referencing of data and/or data sources	Incomplete analysis would not allow full understanding of any performance differences between the current and expected IT environment
Inadequate comparison of the contents of monitoring data to SLAs	Incomplete analysis would not allow full understanding of any performance differences between the current and expected IT environment
Inaccurate reports	Organization acts on inaccurate data

## 1.2 INVESTIGATE AND REMEDIATE PROCEDURE FLOW



### 1.2 Investigate and Remediate Entry Criteria – Availability Management

<b>Inputs</b>	<ul style="list-style-type: none"><li>• Outage Record</li><li>• Missed service availability report</li></ul>
---------------	--

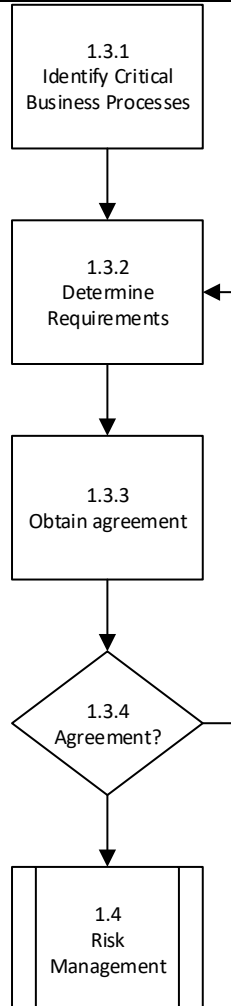
1.2 Investigate and Remediate Entry Criteria – Availability Management	
Entry Criteria	<ul style="list-style-type: none"><li>• Service needing investigation/remediation</li></ul>
General Comments	<ul style="list-style-type: none"><li>• The purpose of this procedure is to ensure review of services with availability misses are investigated and remediated</li></ul>

1.2 Investigate and Remediate Narrative		
Step	Responsible Role	Action
1.2.1	Availability Manager	Identify the Service to be investigated from the Outage Record
1.2.2	Availability Manager	Are there dependencies for the Service that also had an Outage? <ul style="list-style-type: none"> <li>If there is a dependency, proceed to step 1.2.3</li> <li>If there are no additional dependencies, proceed to step 1.2.4</li> </ul>
1.2.3	Availability Manager	Determine if the dependency also impacted an additional service and include in investigation
1.2.4	Availability Manager	Identify cause, frequency and underlying cause of service interruption.
1.2.5	Availability Manager	Has the average availability target been missed against the SLA of more than 30 days? <ul style="list-style-type: none"> <li>If the target average is missed for more than 30 days, proceed to step 1.2.6</li> <li>If the target average has not missed for more than 30 days, proceed to step 1.2.1</li> </ul>
1.2.6	Availability Manager/ SLA Manager	Escalate missed SLA information to the SLA Manager.
1.2 Investigate and Remediate Exit Criteria, Outputs		
Outputs	<ul style="list-style-type: none"> <li>Problem Record</li> </ul>	
Exit Criteria	<ul style="list-style-type: none"> <li>Problem Record created with Availability information</li> </ul>	

<b>1.2 Investigate and Remediate Risks</b>	
<b>Risk</b>	<b>Impact</b>
Business-level Availability Requirements are flawed	Recommendations based on Business-level Availability Requirements are flawed and changes made to the IT environment are inappropriate
Inaccurate understanding of new Plans and/or strategies	Incomplete understanding of potential impacts on the IT environment Incomplete recommendations to improve the IT environment
Service-level Availability Requirements are flawed	Recommendations based on Service-level Availability Requirements are flawed and changes made to the IT environment are inappropriate
Availability Management are not engaged in discussions regarding new or revised SLA, OLA, or UC, or new or changed IT Service	Availability considerations not fully understood Availability requirements not implemented
Inaccurate understanding of new or amended SLAs, OLAs, or UCs, or new or changed IT Services	Incomplete understanding of potential impacts on the IT environment Incomplete recommendations to improve the IT environment
Component-level Availability Requirements are flawed	Recommendations based on Component Availability Requirements are flawed and changes made to the IT environment are inappropriate
Inaccurate understanding of the impact of the introduction of the new/amended Configuration Item	Incomplete understanding of potential impacts on the IT environment Incomplete recommendations to improve IT environment
Business-level Availability Requirements are flawed	Recommendations based on Business-level Availability Requirements are flawed and changes made to the IT environment are inappropriate



### 1.3 PLAN AND DESIGN PROCEDURE FLOW



#### 1.3 Plan and Design Entry Criteria – Availability Management

<b>Inputs</b>	<ul style="list-style-type: none"><li>• Business Plan</li><li>• IT Plan</li><li>• Historical Availability data and information</li><li>• Configuration information</li><li>• SLAs, OLAs, UCs</li><li>• RFC</li></ul>
<b>Entry Criteria</b>	<ul style="list-style-type: none"><li>• New or amended Business Plan or strategy</li><li>• New or amended IT Plan or strategy</li><li>• New or amended IT Service(s)</li><li>• New or amended SLA, OLA, or UC</li><li>• A RFC that will cause the introduction of or amendment to an existing CI</li></ul>

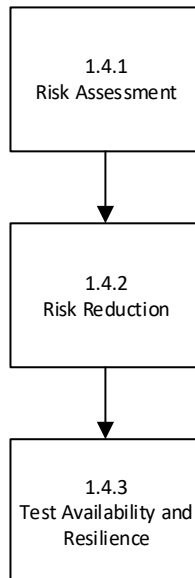
1.3 Plan and Design Entry Criteria – Availability Management	
<b>General Comments</b>	<ul style="list-style-type: none"><li>• Involvement with the business to understand longer-term strategic and shorter-term tactical initiatives, and translating these initiatives into IT environment requirements.</li></ul>

1.3 Plan and Design Narrative		
Step	Responsible Role	Action
1.3.1	Availability Manager/Service Owner	Identify the Critical Business Processes and their associated Availability Requirements in conjunction with the <b>Business Representative</b> and <b>IT Service Continuity Management</b>
1.3.2	Availability Manager/Service Owner	Determine the availability requirements from the business for a new or enhanced IT service and formulate the availability and recovery design criteria. Reference Appendix 4
1.3.3	Availability Manager/ Service Owner	Obtain agreement with the Business Representative and Computing Representative in regard to probability of failure, recovery time, recovery procedures, component availability designs and availability requirements
1.3.4	Availability Manager/ Service Owner	Have Availability requirements been agreed to? <ul style="list-style-type: none"> <li>• If Yes, proceed to 1.4</li> <li>• If No, return to step 1.3.2</li> </ul>

Document New Requirements Exit Criteria, Outputs	
<b>Outputs</b>	<ul style="list-style-type: none"> <li>• Availability Requirements have been documented</li> </ul>
<b>Exit Criteria</b>	<ul style="list-style-type: none"> <li>• Availability Requirements</li> </ul>

<b>Document New Requirements Risks</b>	
<b>Risk</b>	<b>Impact</b>
Business-level Availability Requirements are flawed	Recommendations based on Business-level Availability Requirements are flawed and changes made to the IT environment are inappropriate
Inaccurate understanding of new Plans and/or strategies	Incomplete understanding of potential impacts on the IT environment Incomplete recommendations to improve the IT environment
Service-level Availability Requirements are flawed	Recommendations based on Service-level Availability Requirements are flawed and changes made to the IT environment are inappropriate
Availability Management are not engaged in discussions regarding new or revised SLA, OLA, or UC, or new or changed IT Service	Availability considerations not fully understood Availability requirements not implemented
Inaccurate understanding of new or amended SLAs, OLAs, or UCs, or new or changed IT Services	Incomplete understanding of potential impacts on the IT environment Incomplete recommendations to improve the IT environment
Component-level Availability Requirements are flawed	Recommendations based on Component Availability Requirements are flawed and changes made to the IT environment are inappropriate
Inaccurate understanding of the impact of the introduction of the new/amended Configuration Item	Incomplete understanding of potential impacts on the IT environment Incomplete recommendations to improve IT environment
Business-level Availability Requirements are flawed	Recommendations based on Business-level Availability Requirements are flawed and changes made to the IT environment are inappropriate

## 1.4 EXECUTE RISK MANAGEMENT FLOW



Execute Risk Management Entry Criteria – Availability Management	
<b>Inputs</b>	<ul style="list-style-type: none"> <li>Availability Requirements</li> </ul>
<b>Entry Criteria</b>	<ul style="list-style-type: none"> <li>New Availability Requirements for a Service</li> </ul>
<b>General Comments</b>	<ul style="list-style-type: none"> <li>Risk assessment is based on the probability and potential impact of an event occurring in terms of IT Service availability, and involves the identification and assessment of the level of the risks (calculated by cross-referencing asset value, levels of threats, and vulnerabilities).</li> </ul>

Execute Risk Management Narrative		
Step	Responsible Role	Action
1.4.1	Availability Manager/Service Owner	Perform a review of the Availability Requirements by comparing against the Assets, Threats and Vulnerabilities to understand the risks
1.4.2	Availability Manager/Service Owner	The identified risks should be addressed through appropriate risk reduction measures
1.4.3	Availability Manager/Service Owner	Work with the Service Owner to determine if test plans need to be developed when the Service is changing

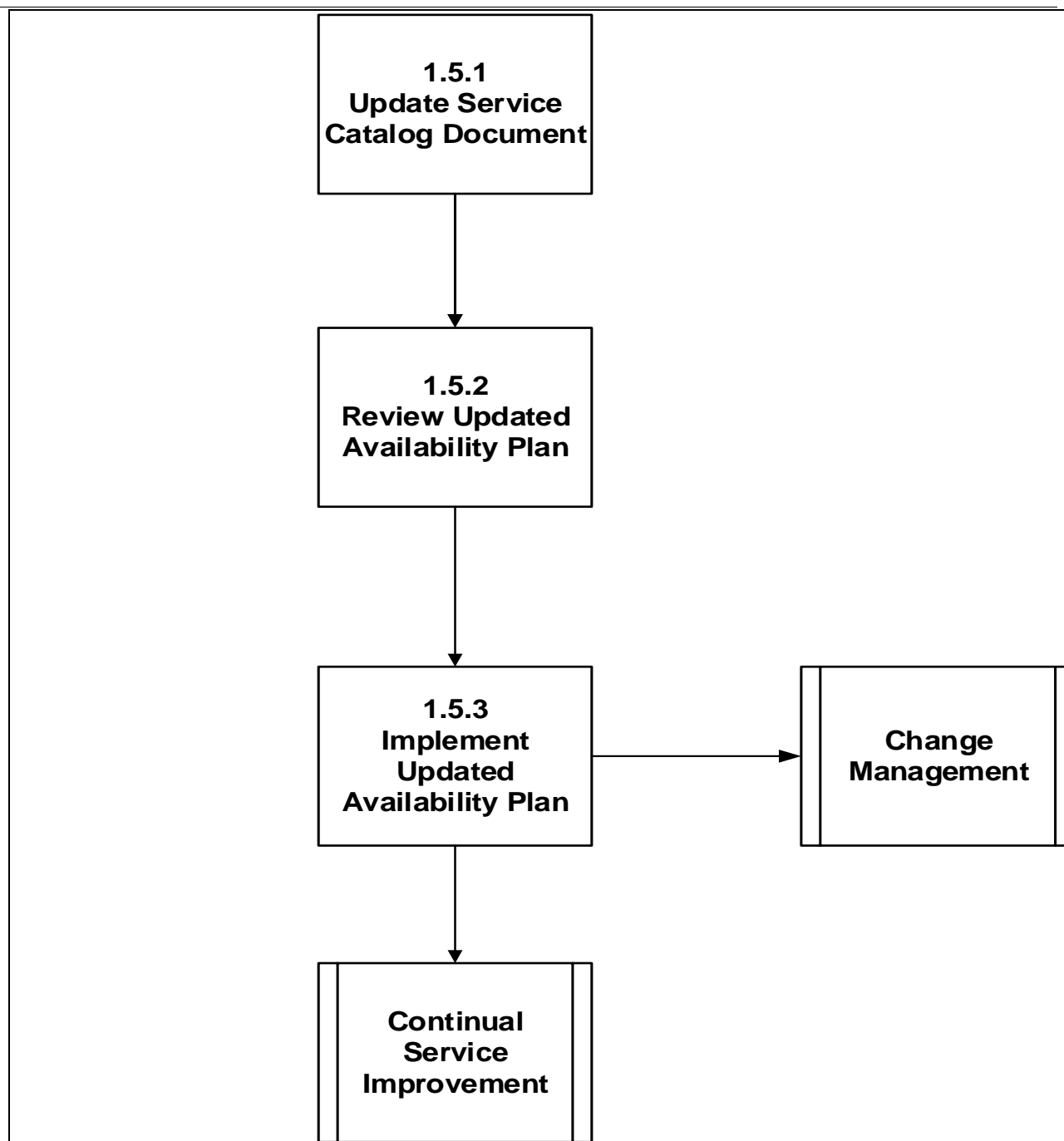
Execute Risk Management Exit Criteria, Outputs	
<b>Outputs</b>	<ul style="list-style-type: none"> <li>Test plans developed for changing services</li> <li>Availability modeling has been completed</li> <li>Availability recommendations have been documented</li> </ul>
<b>Exit Criteria</b>	<ul style="list-style-type: none"> <li>Identified risks and countermeasures</li> <li>Identified vulnerabilities and their levels accurately assessed</li> <li>Identified threats and their levels accurately assessed</li> <li>Validation of the final design to meet the minimum levels of availability</li> <li>Availability recommendations</li> </ul>

<b>Execute Risk Management Risks</b>	
<b>Risk</b>	<b>Impact</b>
Single Point of Failure (SPoF) analysis recommendations are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Identified risks and countermeasures are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Identified vulnerabilities and their levels are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Identified threats and their levels are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Documented IT Services at risk from enabling-Component failure are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Documented impacts of component failure on the business operation and users are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Documented component and people dependencies are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Documented component recovery timings are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Documented alternatives that are available should a CI fail are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Recommendations regarding additional resilience to prevent or minimize the impact of component failure are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Recommendations regarding the need to identify and document recovery options are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Recommendations regarding the need to identify and implement risk reduction measures are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Recommendations to increase the reliability of components are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Recommendations regarding scheduling and performing required internal component maintenance are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Recommendations regarding scheduling and managing required external component maintenance are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate

<b>Execute Risk Management Risks</b>	
<b>Risk</b>	<b>Impact</b>
Recommendations based on the analysis of the impact on IT Service availability arising from component failures are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Security recommendations are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Design recommendations are flawed	Subsequent decisions are flawed and changes made to the IT environment are inappropriate
Availability testing is flawed	Decisions based on testing recommendations are flawed and changes made to the IT environment are inappropriate
Availability modeling is flawed	Decisions based on modeling recommendations are flawed and changes made to the IT environment are inappropriate

## 1.5 SERVICE CAPABILITIES FLOW





Implement New Availability Entry Criteria – Availability Management	
<b>Inputs</b>	<ul style="list-style-type: none"> <li>• Availability analysis recommendations from all previous procedures</li> <li>• Identified risks and countermeasures, vulnerabilities, threats</li> <li>• Availability test results</li> <li>• Availability modeling results</li> <li>• Updated Availability maintenance schedule</li> <li>• Availability Requirements</li> </ul>
<b>Entry Criteria</b>	<ul style="list-style-type: none"> <li>• Business-level Availability Requirements, Service-level Availability Requirements and Component-level Availability Requirements have been documented</li> </ul>
<b>General Comments</b>	<ul style="list-style-type: none"> <li>• The Service Catalog Document produced annually at predefined intervals in line with the business or budget life cycle and updates to the Service Catalog Document can also be triggered as the result of a significant change in business needs.</li> </ul>

Implement New Availability Narrative		
Step	Responsible Role	Action
1.5.1	Availability Manager	Evaluate elements of the previous Service Catalog Document for continuation, modification, or exclusion and compare to the recommendations/updates.
1.5.2	Availability Manager	Proceed to update the Service Catalog Document with the recommendations/updates
1.5.3	Availability Manager	Implement the updates to the Service Catalog Document in Service Now and correlate with a Change
<p><b>Note:</b> At this point, with the New Service Catalog Document developed and deployed, the data is available to allow for entry into the <b>Continual Service Improvement Process</b>. The process can be analyzed and opportunities for improvement identified.</p>		

Implement New Availability Exit Criteria, Outputs	
<b>Outputs</b>	<ul style="list-style-type: none"> <li>• Updates have been made to the Service Catalog Document</li> <li>• Requests For Change are created and submitted to the Change Management process</li> </ul>

<b>Exit Criteria</b>	<ul style="list-style-type: none"><li>• Updated Service Catalog Document</li><li>• Request(s) For Change</li></ul>
----------------------	--

Implement New Availability Risks	
Risk	Impact
Recommendations are created from inaccurate data	Recommendations are flawed and changes made to the IT environment are inappropriate
Not all recommendations are included in the Service Catalog Document	Recommendations are flawed and changes made to the IT environment are inappropriate
Recommendation does not get turned into a RFC	Improvements to the IT environment are not undertaken




<b>PROCESS INTEGRATION POINTS – AVAILABILITY MANAGEMENT</b>			
<b>Process</b>		<b>Process</b>	<b>Information</b>
Availability Management	to	Incident Management	<ul style="list-style-type: none"> <li>Availability design for solutions to Incidents</li> </ul>
Incident Management	to	Availability Management	<ul style="list-style-type: none"> <li>Reports of incidents affecting Availability and related Incident data</li> </ul>
Availability Management	to	Problem Management	<ul style="list-style-type: none"> <li>Availability reports to indicate current or future Problems</li> <li>Propose Solutions to Availability Problems</li> </ul>
Problem Management	to	Availability Management	<ul style="list-style-type: none"> <li>Report of availability related problems and known errors</li> <li>Progress reports of Problems related to Availability Problem data</li> </ul>
Availability Management	to	Change Management	<ul style="list-style-type: none"> <li>Submit Change Requests for Change (RFCs)</li> <li>Advise on CRs</li> <li>Assists in identifying impact of Changes on Projected Service Availability (PSA)</li> <li>Planned Service Outages for tests and preventative maintenance</li> </ul>
Change Management	to	Availability Management	<ul style="list-style-type: none"> <li>Post Implementation Review - Change impact on Availability</li> <li>Change Schedule</li> <li>Include Availability Management in CAB</li> <li>Backed out changes</li> <li>Projected Service Availability (PSA) for agreement – confirmation</li> </ul>
Availability Management	to	Service Level Management	<ul style="list-style-type: none"> <li>SLM/O/R achievement reports</li> <li>Coordinate with SLM to provide proper Service Level Agreement (SLA) targets</li> </ul>
Service Level Management	to	Availability Management	<ul style="list-style-type: none"> <li>Service Level Requirements, SLA's, Operating Level Agreements (OLA's), Underpinning Contracts (UC's)</li> <li>Service Catalog</li> </ul>
Availability Management	to	Capacity Management	<ul style="list-style-type: none"> <li>Availability data and metrics reporting</li> <li>Resiliency requirements of availability targets</li> </ul>
Capacity Management	to	Availability Management	<ul style="list-style-type: none"> <li>Provide Availability requirements of the Capacity Plan</li> <li>Provide Capacity schedules for AM to plan and integrate effectively with Capacity Management</li> <li>Details of new technology being considered</li> </ul>
Availability Management	to	Financial Management	<ul style="list-style-type: none"> <li>Details of unavailability events</li> </ul>

<b>PROCESS INTEGRATION POINTS – AVAILABILITY MANAGEMENT</b>			
<b>Process</b>		<b>Process</b>	<b>Information</b>
Financial Management	to	Availability Management	<ul style="list-style-type: none"> <li>Cost of service unavailability to include (where applicable):               <ul style="list-style-type: none"> <li>Lost user and IT productivity</li> <li>Lost revenue</li> <li>Overtime payments</li> <li>Wasted goods and materials</li> <li>Imposed fines and penalties</li> <li>Loss of goodwill or customers</li> </ul> </li> </ul>
Availability Management	to	Configuration Management	<ul style="list-style-type: none"> <li>Updates to important relationship between CIs; resilience</li> </ul>
Configuration Management	to	Availability Management	<ul style="list-style-type: none"> <li>CI relationship data used to establish users affected by availability and identify viable alternatives if Availability issues arise</li> <li>Details of CIs that need to be risk managed as part of Availability Plan</li> </ul>
Availability Management	to	Release Management	<ul style="list-style-type: none"> <li>Availability test schedule</li> </ul>
Release Management	to	Availability Management	<ul style="list-style-type: none"> <li>Release schedule</li> </ul>
Availability Management	to	IT Service Continuity Management (ITSCM)	<ul style="list-style-type: none"> <li>Risk analysis and risk assessment information to ITSCM to enable a better understanding of the risks involved during different scenarios</li> <li>Design criteria for new and changed services</li> </ul>
ITSCM	to	Availability Management	<ul style="list-style-type: none"> <li>Business Impact Analysis</li> <li>Availability requirements of the Service Continuity plans</li> <li>Service continuity and contingency plans to support the Availability management process.</li> <li>Risk Management and risk analysis to Availability Management</li> <li>Standby options that Availability Management needs to be aware of when developing Availability Plans</li> </ul>

SUPPORTING DOCUMENTS		
Document Name	Description	Relationship
Availability Management Business Process Requirements	Requirements	Availability Management Business Process Requirements
Service Improvement Process & Procedures	Process, Procedure	Service Improvement Process & Procedures
Change Management Process & Procedure	Process, Procedure	Change Management Process & Procedure

## APPENDIX 1 - AVAILABILITY RACI MATRIX

**R - Responsible** Person responsible for getting the work done  
**A - Accountable** Only one person can be accountable for each activity  
**C - Consult** The people who are consulted and whose opinions are sought  
**I - Inform** The people who are kept up-to-date on progress

 Primary Roles in Process  
 Primary Interactions  
 Secondary Roles

Procedures and Activities	Availability Manager	Problem Manager	Incident Manager	Capacity Manager	Continuity Manager	Service Level Manager	Tier 2 Support	Process Owner	Customer
<b>Monitor and Review</b>									
1.1 – Monitor and Review	R	C	C	C			R	A	I
1.17 – Create Outage Records	R	C	C	C		C	C	A	I
<b>Investigate and Remediate</b>									
1.2.2 – Determine Service Dependencies	R		C		C		C	A	
1.2.4 – Identify cause, frequency, underlying cause	R	R	C	C	I	C	C	A	
1.2.6 – Escalation to Service Level Manager	R	C	R	C		A	C	I	
<b>Plan and Design</b>									
1.3.1 – Identify Critical Business Processes	A	I	I	C	C	R		C	C
1.3.2 – Determine Service Availability Requirements	A	I	I	C	C	R		C	C
1.3.3 – Obtain agreement on Availability Requirements	A	I	I	C	C	R		C	C
<b>Risk Management</b>									
1.4.1 – Perform Risk Analysis and Management	R	C	C	C		C		A	

1.4.2 – Design for Availability	R			C	I	C	C	A	
1.4.3 – Manage Availability Testing	R	I	I	C	C			A	I
Service Capabilities									
1.5.1 - Create Updates to Availability Plan	R	C	C	C	C	C	C	A	C
1.5.2 - Review Updated Availability Plan	R	C	C	C	C	C	C	A	C
1.5.3 - Implement Updated Availability Plan	R							A	I



## APPENDIX 2 – COMMUNICATION

This document describes a plan for communicating the Computing Sector's Availability Management policy, process, procedures, techniques and use of associated tools to the Computing community.

### 2.0 MANAGEMENT COMMUNICATION

The Availability Management process requires communication to the management team, covering:

- Status of issues regarding the unavailability of services and service-enabling infrastructure components.
- Relevant Key Performance Indicators (KPIs) to measure the performance of the process.
- Watch list of issues of interest that may impact service availability.
- Continual Service Improvement Process (CSIP) initiatives: their descriptions, owners, plans, expectations and status.

The methods of communication for current availability issues will be:

- Presentation of written reports at some Computing Sector Operations meetings,
- Sending operations reports to management by the Computing Sector Operations email list,
- Targeted emails, instant and text messages, phone calls, or visits to inform management of the status of critical issues as appropriate.

KPIs and CSIP will be communicated by:

- Presenting written reports at the Service Management Operations meeting,
- Sending Service Management Operations report to management via the Service Management Operation email list.

### 3.0 OVERALL COMMUNICATION

The Availability Management process requires communication to the other ITIL process owners and with service providers and their respective support teams to gather information and coordinate efforts.

#### 3.1 ONGOING COMMUNICATION

The Availability Manager has the ability to set review meetings as needed, particularly in the investigation of issues that impact service availability.

The Availability Manager has the ability to call planning meetings for preparing the Availability Plan.

The Availability Manager has the ability to call meetings to investigate approaches and techniques for improving availability.

The Availability Manager will provide routine status updates to interested parties as appropriate. Awareness and Training will be provided as needed, including at the implementation of major changes to the process, techniques or the use of associated tools

Methods of communication:

- Targeted emails, instant and text messages, phone calls, or visits to update management on status of critical investigations as appropriate
- Availability Review or status and planning meetings with Availability Analysts

### APPENDIX 3 - DEFINITIONS

Term	Definition
Availability	The percentage of the agreed service hours for which the component or service is available.
Reliability	The prevention of operational failure, and the ability to keep services and IT infrastructure components operable
Maintainability	The ability to restore services or IT infrastructure components back to normal operation
Serviceability	Defines the contractual agreements made with external suppliers. These are to assure the availability, reliability and maintainability of services' IT infrastructure components under external suppliers' care
Security	The integrity, confidentiality and availability of data associated with a service
SLA	Service Level Agreement - A written agreement between a service provider and Customer(s) that documents agreed service levels for a service.
Vital Business Function	Represents a business-critical element of a business process supported by an IT service
High Availability	A characteristic of IT Service that minimizes the effects of component failure to the Customer (User)
Continuous Operation	A characteristic of IT Service that minimizes that effects of planned down-time to the Customer (User)
Continuous Availability	A characteristic of IT Service that minimizes the effects of all failures and planned downtime to Customer (User)

### APPENDIX 4 – ISO REQUIREMENTS

Section	Requirement	Intent Documentation	Evidence Location

6.3.1	The service provider <b>SHALL</b> assess and document the risks to service continuity and availability of services.	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document
6.3.1	The service provider <b>SHALL</b> identify and agree with the customer and interested parties service continuity and availability requirements.	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document
6.3.1	The agreed requirements <b>SHALL</b> take into consideration applicable business plans, service requirements, SLAs and risks.	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document
6.3.1	The agreed service continuity and availability requirements <b>SHALL</b> include at least:	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document
6.3.1	a) access rights to the services;	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document
6.3.1	b) service response times;	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document
6.3.1	c) end to end availability of services.	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document
6.3.2	The service provider <b>SHALL</b> create, implement and maintain a service continuity plan(s) and an availability plan(s).	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document

6.3.2	Changes to these plans <b>SHALL</b> be controlled by the change management process.	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document
6.3.2	The availability plan(s) <b>SHALL</b> include at least availability requirements and targets.	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document
6.3.2	The service provider <b>SHALL</b> assess the impact of requests for change on the service continuity plan(s) and the availability plan(s).	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document
6.3.2	NOTE The service continuity plan(s) and availability plan(s) can be combined into one document.	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document
6.3.3	Availability of services <b>SHALL</b> be monitored, the results recorded and compared with agreed targets.	Availability Management Process & Procedures (DocDB #4083)	Outage records in Service Now
6.3.3	Unplanned non-availability <b>SHALL</b> be investigated and necessary actions taken.	Availability Management Process & Procedures (DocDB #4083)	Outage records in Service Now
6.3.3	Availability plans <b>SHALL</b> be tested against the availability requirements.	Availability Management Process & Procedures (DocDB #4083)	Service Catalog Document
6.3.3	Service continuity and availability plans <b>SHALL</b> be re-tested after major changes to the service environment in which the service provider operates.	Availability Management Process & Procedures (DocDB #4083)	Service Now Dashboards
6.3.3	The results of the tests <b>SHALL</b> be recorded.	Availability Management Process & Procedures (DocDB #4083)	Major Service Now Changes